Rajat Tambare, 2021, 9:3
ISSN (Online): 2348-4098
ISSN (Print): 2395-4752

Electoblock: A Secure Digital Voting System Based on Blockchain Technology

Rajat Tambare, Prajakta Dixit, Raghavendra Singh Gehlot
Department of Computer Science
Acropolis Institute of Technology and Research,
Indore, MP,India
Rajiv Gandhi Technical University, Bhopal.

Abstract- Voting is the fundamental right for every nation. An Electronic Voting (E-Voting) system is a voting system in which the election process is notated, saved, stored, and processed digitally, which makes the voting management task better than the traditional paper-based method. Blockchain is offering new opportunities to develop new types of digital services. While research on the topic is still emerging, It has mostly focused on the technical and legal issues instead of taking advantage of this novel concept and creating advanced digital services. Blockchain-enabled e-voting (BEV) could reduce voter fraud and increase voter access. Eligible voters cast a ballot anonymously using a computer or smart phone. BEV uses an encrypted key and tamper-proof personal IDs. Electronic credibility services have become an integral part of the information space. With the reliable implementation of basic services as an electronic signature and electronic authentication, it is possible to build more complex systems that rely on them, particularly the electronic voting system. This paper presents the concept of developing an electronic voting system using blockchain technology. The two-level architecture provides a secure voting process without redundancy of existing (not based on blockchain) systems. The blockchain-based voting system has two modules to make the whole process integrated and work along. One will be the Election Commission who will be responsible for creating elections, adding registered parties and candidates contesting for the election added under the smart contracts. The other end will be the voter's module where each individual can cast a vote for their respective Assembly Constituency and the vote will be registered on the blockchain to make it tamper proof.

Keywords:- Matlab, OpenCV, Faster-RCNN, Convolutional neural network, COCO.

I. INTRODUCTION

Modern democracies are built upon traditional ballot or electronic voting (e- voting). In these recent years, devices which are known as EVMs are hugely criticized due to irregular reports of the election results. There have been many questions regarding the design and internal architecture of these devices and how it might be susceptible to attacks. This [1] paper has analyzed different techniques of tampering the EVMs. Online-voting is pushed as a potential solution to attract the young citizens and the non- resident of the country. For a robust online election scheme, a number of functional and security requirements are to be met such as transparency, accuracy, data privacy, etc.

We have worked the following ideas by having the two different set of modules: election commission and the voter(s). Election Commission creates elections and adds registered candidates along with the parties for contesting the election. Using an election's REST API hosted on Ethereum's Blockchain, the details are shown at the front-end of the voter

for casting the vote. Then, while polling the vote is stored on our blockchain framework of which the Election Commission fetches the vote count. The limitation which we have faced due to not using the traditional way of smart contracts is that the blockchain framework which we have coded cannot run on the main net as it needs to be hosted and a separate web3 provider have to be used for interacting with it and not having a public API of voter ID creates a drawback of not having authentication of a voter.

II. ELECTRONIC-VOTING SYSTEM

Electronic voting, a form of computer-mediated voting in which voters make their selections with the aid of a computer. The voter usually chooses with the aid of a touch-screen display, although audio interfaces can be made available for voters with visual disabilities. The computer which is used in electronic voting system is known as electronic voting machine or EVM.

Electronic Voting Machine (EVM's) mainly consists of two components:

1. **Control Unit:** It stores and assembles votes, used by poll workers.
2. **Ballot Unit:** It is placed in the election booth and is used the voters.

Both the units are connected via 5m cable and one end of the cable is permanently fixed to ballot unit. The control unit has a battery pack inside, which motorizes the system. The ballot unit has 16 candidate button and the unused buttons are covered with a plastic masking tab inside the unit. An additional ballot unit can be connected when there are more than 16 candidates.

The additional ballot unit can be connected to a port on the underside of the first ballot unit. EVM's are internationally known as DRE's (Direct recording Electronic). By using EVM's, Votes are correctly recorded and there is no problem in counting, scalability,

Accuracy, fast declaration of results and robustness of system. Main Problem lies in authentication, the person who is voting may not be the legitimate person. Other problems like capturing of booth by political parties, casting of votes by underage people and fraud voting may occur.

A person is provided with the voter ID card as a proof of identity, issued by Indian government. Lot of problems are seen in voter id cards like name misprinting, missing of name, no clear photo on photo id card etc.

In today's world, distributed ledger technologies such as blockchain have been used in e-voting systems because blockchain have various advantages in terms of end-to-end verifiability.

Many properties such as security, verifiability, anonymity, privacy protection are present in blockchain. Because of such properties it can be a very effective and attractive alternative to the old e-voting systems.The research presented in this paper also attempts to show these properties of blockchain to achieve more efficient e-voting system than existing one.

III. REQUIREMENTS OF ELECTRONIC-VOTING

In this section, we present a detailed description of each requirement along with the explanation of how our proposed system fulfils it.

1. Privacy:
Privacy is one of the most important aspects of democratic voting. Voter's privacy should be maintained. No one should be able to know how a particular person voted or to whom the particular voter voted.

2. Eligibility:
This property states that only eligible users can vote. Those who are provided with authentication by the Election Commission.

3. Coercion Resistance:
No one should be able to force the voter and should not have the ability to distinguish between whether the voter voted the same way he/she was instructed to vote.

4. Verifiability:
This property states that everyone involved in the voting process should be able to verify the results. This brings transparency in the election. Also, an individual voter should be able to verify whether his/her vote is counted or not.

International Journal of Science, Engineering and Technology

An Open Access Journal

IV. RELATED WORKS

In this section, we present some of the related works in the electronic-voting systems that use blockchain.

Agora is an end-to-end blockchain based voting solution designed for governments. Agora uses their own Token on the blockchain for elections, where governments and institutions purchase these tokens for each individual eligible voter.

A Smart Contract for Boardroom Voting with Maximum Voter Privacy, proposed the first implementation of a decentralized and self-tallying internet voting protocol. It has maximum voter privacy using the Blockchain. The Open Vote Network (OVN) is written as a smart contract on the public Ethereum blockchain.

Digital Voting with the use of Blockchain Technology proposed an integration of the blockchain technology to the current voting system in the UK. In which the voters can vote at a voting district or on a web browser at home.

Netvote which is a decentralized blockchain-based voting network. It can run on the Ethereum blockchain. Netvote utilizes decentralized apps for the user interface of the system.

The Admin decentralized app (dApp) allows election administrators to set election policies, create ballots, establish registration rules and open and close voting. The Voter dApp is used by individual voters for registration, voting and can be integrated with other devices (such as biometric readers) for voter identification. The Tally dApp is then used to count and verify election results.

The focus of this research is to explore the exciting opportunities of blockchain technologies by investigating their application in diverse application domains. This paper presents our efforts to develop an e-voting system by leveraging blockchain technology.

V. PROPOSED SYSTEM DEISGN

The proposed e-voting system is called ElectoBlock a web application. It can help in implementing an electronic voting system which is immutable, transparent and cannot be hacked into in order to change the results. The system has been designed to support a voting application in the real world environment taking into account specific requirements such as privacy, eligibility, convenience, receipt- freeness and verifiability. The proposed system aims to achieve secure digital voting without compromising its usability.

Within this context, the system is designed using a web-based interface to facilitate user engagement. Furthermore, the system allows all voter's equal rights of participation and develops a fair and healthy competition among all the candidates while keeping the anonymity of the voters preserved.

The proposed system is divides into following modules:-

1. **Election Commission:**

In this module, an entity named Election Commission will be responsible to setup the smart contract and register candidates, parties and start off an election.

2. **Election Test:**

This is the module to test our smart contract where we use Mocha Framework to perform unit test on our application.

3. **Voter Module:**

In this module, voters who have been provided with the personal ETH wallet will import onto the voting portal using the Metamask extension and cast their vote.

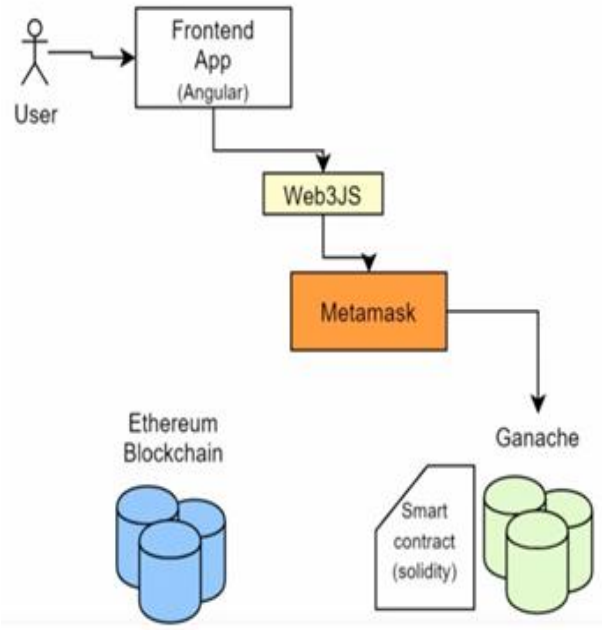

Fig 1. Software Architecture.

International Journal of Science, Engineering and Technology

An Open Access Journal

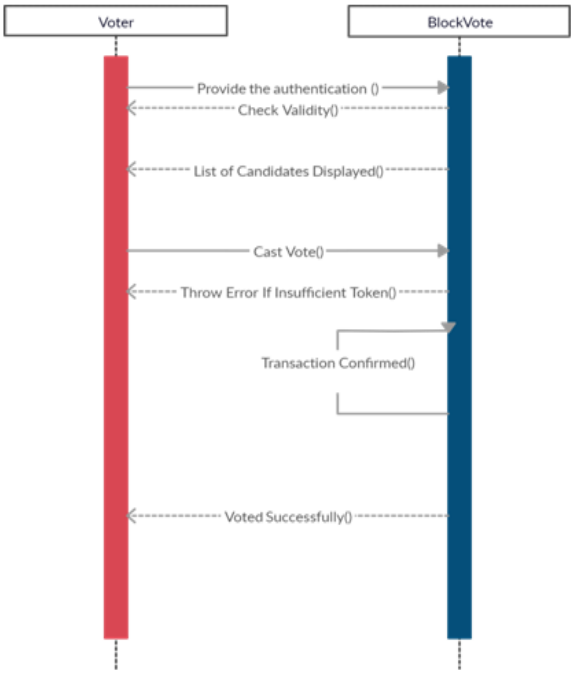

Fig 2. Sequence Diagram.

4. The Voting Process:

We now describe the interaction of a user or voter with the proposed scheme based on our current implementation of the system. Typically, a voter logs into his metamask account using the private key provided by the election commission after successful verification. After successful login, the voter is then presented with a list of available candidates with the option to cast vote against them.

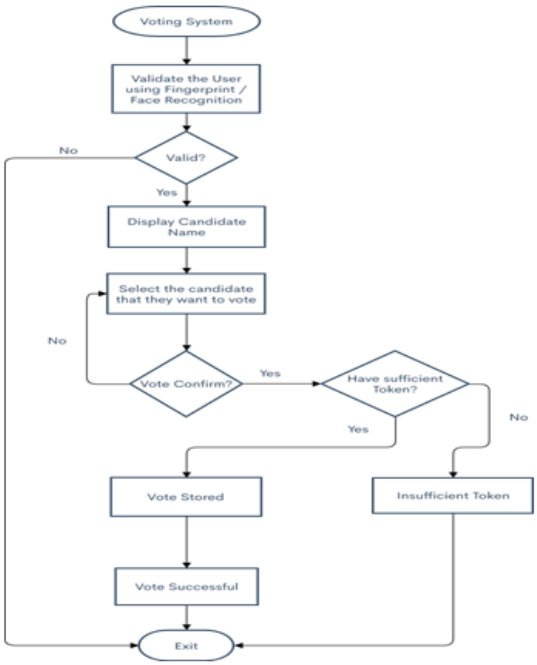

Fig 3. Flowchart.

In this system all the authentication process is done prior to the election by election commission and private key is provided to all potential voters after successful verification. After a successful vote-cast a new block is added to the blockchain. After this it cannot be changed. This makes this system very secure.

VI. CONCLUSION

Democracies depend on trusted elections and citizens should trust the election system for a strong democracy. However traditional paper-based elections do not provide trustworthiness. The idea of adapting digital voting systems to make the public electoral process cheaper, faster and easier, is a compelling one in modern society.

Making the electoral process cheap and quick, normalizes it in the eyes of the voters, removes a certain power barrier between the voter and the elected official and puts a certain amount of pressure on the elected official. It also opens the door for a more direct form of democracy, allowing voters to express their will on individual bills and propositions.

In this paper, we introduced a blockchain-based electronic voting system that utilizes smart contracts to enable secure and cost-efficient election while guaranteeing voters privacy. We have shown that the blockchain technology gives us a new possibility to overcome the drawbacks of electronic voting systems which ensures the election security, integrity and transparency.

REFERENCES

[1] Wolchok, Scott, et al. "Security analysis of India's electronic voting machines." Proceedings of the 17th ACM conference on Computer and communications security. ACM, 2010.

[2] Ohlin, Jens David. "Did Russian cyber interference in the 2016 election violate international law." Tex. L. Rev. 95 (2016): 1579.

[3] Ayed, Ahmed Ben. "A conceptual secure blockchain-based electronic voting system." International Journal of Network Security & Its Applications 9.3 (2017): 01-09.

[4] Hanifatunnisa, Rifa, and Budi Rahardjo. "Blockchain based e-voting recording system design." 2017 11th International Conference on

International Journal of Science, Engineering and Technology

An Open Access Journal

Telecommunication Systems Services and Applications (TSSA). IEEE, 2017.

[5] Yu, Bin, et al. "Platform-independent secure blockchain-based voting system." International Conference on Information Security. Springer, Cham, 2018.